APPENDIX A

Version with Markings
to Show Changes Made to the Claims

The following are marked up versions of the amended Claims:

1.(TWICE AMENDED) A security token comprising:

a biometric sensor that provides a first biometric key of a current user of the security token, based upon a biometric measure of the current user,

a storage element that stores an encryption of a security key, the encryption being based on a second biometric key of an authorized user,

a biometric decrypter, operably coupled to the biometric sensor and the storage element, that decrypts the encryption of the security key with the first biometric key, producing thereby a decrypted security key[that is equal to the security key when the first biometric key is equivalent to the second biometric key], and

an authentication encrypter, operably coupled to the biometric decrypter, that encrypts a received challenge parameter with the decrypted security key to produce a response parameter[that is based upon the decrypted security key].

9.(TWICE AMENDED) A security system comprising:

a token that includes:

a biometric sensor that provides a first biometric key of a current user of the token based upon a biometric measure of the current user,

an encryption of a security key, the encryption being based upon a second biometric key of an authorized user, and

a biometric decrypter that decrypts the encryption of the security key to produce a decrypted security key using the first biometric key, such that

the decrypted security key is equivalent to the security key when the first biometric key is equivalent to the second biometric key,

the decrypted security key is an erroneous key when the first biometric key is different from the second biometric key; and

an authentication encrypter, operably coupled to the biometric decrypter, that encrypts a challenge parameter to produce a response parameter that is based upon the decrypted security key; and

an access device that, when operably coupled to the token, determines an access status based upon the [decrypted security key]response parameter.

18.(THRICE AMENDED) A method for determining an access status comprising the steps of:

enabling encrypting a security key to produce an encrypted security key based upon a first biometric key of an authorized user into a token,

enabling determining a second biometric key of a current user of the token based upon a biometric measure of the current user,

enabling decrypting the encrypted security key to produce a decrypted security key based upon the second biometric measure,[and]

enabling the token to receive a challenge parameter,

enabling encrypting the challenge parameter with the decrypted security key to produce an encrypted challenge parameter; and

enabling determining an access status based upon the [decrypted security key and the response parameter]encrypted challenge parameter.

20.(THRICE AMENDED) The method of Claim 18, wherein

the security key is a first key of a pair of symmetric keys, and

[the step of determining the response parameter includes the step of encrypting the challenge parameter based upon the second biometric key, and]

the step of determining the access status includes the steps of:

decrypting the [response parameter]encrypted challenge parameter[to produce a decrypted result based upon] with a second key of the pair of symmetric keys to produce a decrypted result, and

comparing the decrypted result to the challenge parameter to determine the access status.